EX PARTE OR LATE FILED

ORIGINAL

WILEY, REIN & FIELDING

1776 K STREET, N.W.
WASHINGTON, D.C. 20006
(202) 429-7000

PETER D. ROSS
(202) 429-4232

December 9, 1998

FACSIMILE
(202) 429-7049

BY HAND

RECEIVED

DEC 10 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Ms. Magalie Roman Salas
Secretary
Federal Communications Commission
1919 M St., N.W. Room 222
Washington, D.C. 20554

Re: Notification of Permitted Written *Ex Parte* Presentation in CC Docket No. 98-146

Dear Ms. Salas:

Pursuant to Section 1.1206(b)(1) of the Commission's rules, attached please find two copies of materials which Mr. Suk S. Soo of America Online, Inc. ("AOL") provided to FCC officials in the course of a December 9, 1998 multi-party meeting organized by FCC Chief Technology Officer Stagg Newman to discuss technical issues in the above-referenced docket. Both documents are publicly available. The first, titled "Third Party Residential Internet Access: Point of Interconnect Network Design," is by Tekton Internet Associated, Inc. The second, titled "Technical Report on the Status of Implementation of Access For Internet Service Providers," was submitted to the Canadian Radio-Television and Telecommunications Commission (CRTC) by the Canadian Cable Television Association (CCTA) in response to Telecom Decision 98-9. The documents describe the technical terms mutually agreed upon by Canadian regulators and cable operators to afford multiple Internet service providers fair access to cable high-speed Internet access networks.

Kindly direct any questions regarding this matter to the undersigned.

Respectfully submitted,

Peter Ross

Peter D. Ross

cc with attachments:
Stagg Newman, Office of Engineering and Technology
Jeffrey Lanning, Office of General Counsel

No. of Copies rec'd 0+1
List ABCDE

TEKTON
Internet Associates

99 Winchester St
Toronto ON
M4X 1B1

416 924 2379
416 924 3279

Third Party Residential Internet Access

Point of Interconnect Network Design

Project:	Third Party Equal Access
Prepared By:	Tekton Internet Associates, Inc.
Authors:	Frank I. Reiter
	Eric M. Carroll
Client:	Barbara Adey, CCTA
Revision Number:	24
Release Date:	11/17/98
Release Status:	RELEASED

Table of Contents

TPRIA Point of Interconnect Network Design

1 Introduction

This document follows and builds on the "Third Party Residential Internet Access Proposed Service Definition" delivered to the CCTA in February of 1998. It describes the network design and implementation of alternative three of the Technical Report on Alternatives submitted to the CRTC by the CCTA on August 24^{th}, 1998.

This document does not address the business processes necessary to support the TPRIA product.

2 Definitions

2.1 Definitions

Cable Network Operator (CNO)

Owner operator of the CATV distribution network. A CNO or its affiliate may also operate as an ISP.

Classless Inter-Domain Routing (CIDR)

CIDR permits allocation of network numbers with the network mask set at nearly any boundary within the IP address field. It supersedes the older practice of allocating IP address space only in class A, class B or class C network blocks. CIDR is now the commonly accepted practice for IP address allocation.

Customer

An Internet Service Provider (ISP) is a customer of the Equal Access service. A Customer offers value-added services to its Subscribers.

Data Over Cable System (DOCS)

For the purposes of this document, a generic term for the infrastructure equipment that implements two-way packet data services over a CATV distribution network.

Dynamic Host Configuration Protocol (DHCP)

A mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them. DHCP is defined in RFC 1541.

Incumbent Network (IN)

The CNO's Internet access service offering.

Internet Service Provider (ISP)

A company (other than the CNO) offering Subscribers access to the Internet and to Internet value-added services, such as electronic mail, network news, and World Wide Web.

Point of Interconnection (POI)

The physical meeting point between the ISP IP network and the CNO's TPRIA DOCS access/distribution network. There is a POI located within the geographic area of each RSAN. Thus, the CNO may operate as many POI's as there are RSAN's within its operating territory.

Subscriber

Residential end-user/consumer of Internet access and other services delivered via the CNO's facilities.

Residential Subscriber Access Network (RSAN)

The TPRIA DOCS infrastructure and its directly connected cable plant within a given geographic locality. In HFC infrastructures, this is also known as the Primary Fibre-Optic distribution hub or Head-end, depending on CNO fiber network architecture, and its subsidiary co-axial cable plant.

3 Service Requirements

The service requirements for this product are documented in detail in the Third Party Residential Internet Access Proposed Service Definition. This section describes additional requirements that became apparent during the creation of this document.

3.1 Subscriber addressing

3.1.1 Subscriber domain name

In order that Subscribers are able to accept incoming IP sessions it is necessary that the domain name assigned to a Subscriber remain unchanged for the duration of the subscription, even if the Subscriber's IP address is changed (see below).

3.1.2 Subscriber IP address

- The Subscriber's IP address is allocated by the CNO from a pool provided by the Customer . The Subscriber need not interact with this address.
- In order to avoid interrupting application sessions and in order to interoperate with current DHCP client implementations the Subscriber's IP address must not change during the course of a boot session.
- It must be possible for the CNO to occasionally change the IP address assigned to Customers on one RSAN. Such changes may require a reboot by affected Subscribers who are using the service at the time of the change but should otherwise be transparent to Subscribers.

4 Design Assumptions and Limitations

4.1 Number of Subscriber PCs

This design assumes that each Subscriber will access the service from just one PC. Additionally, the PC used to access this service will be assigned an IP address dynamically by the CNO. This will complicate communication between this PC and any other PC on the Subscriber's LAN.

4.2 DHCP Client Identification

This document assumes that DHCP clients (modems and Subscriber PCs) are identified by their MAC address and not by a configurable client ID, which would also be possible with DHCP. Each approach has different challenges - only those associated with using MAC addresses are addressed in this document.

4.3 Reliance on DHCP

This service relies on the ability of the Subscriber's PC to function as a DHCP client. Platforms incapable of doing so are not supported by this service.

4.4 Collection of Billing Data

Billing model metrics (IE, a list of the things that trigger charges to the Customer) were not available as input to this report. This report therefor does not address the collection of the information which will be used as a basis for billing. Charges to the Customer may include the following:

- Customer signup fee
- POI connection installation fee
- POI connection monthly fee
- Data backhaul fees
- Bandwidth utilization fee
- Subscriber installation fee
- Subscriber monthly fee

4.5 POI Routers Not Transit Points

Some outbound Subscriber traffic may be destined for an ISP which is not the one serving that Subscriber, but which is connected to the same POI router. It might seem natural in that case to pass the traffic directly on to that second ISP rather than routing it to the Subscriber's ISP.

Supporting this ability would require the CNO to become an N-way connected autonomous system, with each POI router maintaining full routing tables for all Customers.

It is a non-trivial task to establish and maintain that ability. In addition, routing on this scale requires routers that are substantially larger than a CNO might otherwise require in many RSANs.

For these reasons, POI routers are explicitly not transit points. This is further discussed in section 5.4, Routing.

5 Functional Design

In this section we propose a design which meets the requirements set out in the "Third Party Residential Internet Access Proposed Service Definition" and in the Service Requirements section of this document

5.1 Logical Network Design

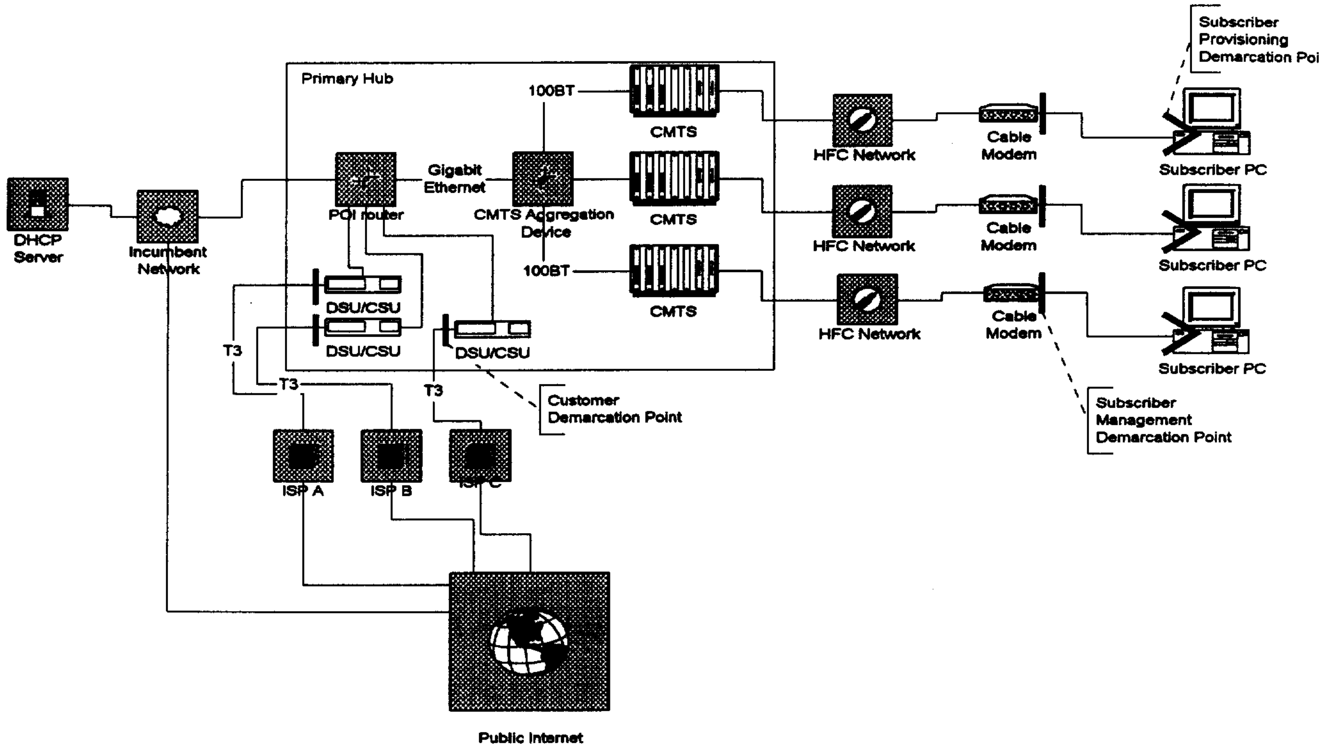
5.1.1 Overview

The logical network design is detailed in Figure 5.1.

Each of the components in Figure 5.1 will be logically present in the network, however multiple logical components may be integrated into one physical device. For example, the CMTS aggregation device may be a fast Ethernet switch connected to multiple discrete CMTS units. Alternatively, a single piece of equipment may perform aggregation and CMTS functions for multiple downstream channels.

Subject to capacity of the specific hardware devices installed, an arbitrary number of Customers may be connected to one POI router, an arbitrary number of CMTSs may be connected to one aggregation device and an arbitrary number of Subscribers may be connected to one CMTS.

Where a POI router serves only one CMTS the two devices may be connected directly to each other without any intervening aggregation device.



TEKTON	TITLE: Equal Access Logical Network Diagram	FILENAME: EA Logical.vsd
	PROJECT: Equal Access - Point of Interconnect	CREATOR: Frank Reiter
	DATE: 10/1/98 TIME: 2:14:57 PM PG: 1 OF 1 PGS	© 1998 Tekton Internet Associates, Ir

• Figure 5.1 Logical Network Design with POI in Primary Hub

5.1.2 Demarcation Points

There are three functional demarcation points in the logical network design as denoted in Figure 5.1:

1. Customer Demarcation Point
2. Subscriber Management Demarcation Point
3. Subscriber Provisioning Demarcation Point

5.1.2.1 Customer Demarcation Point

The customer demarcation point is the point closest to the POI at which the Customer will actively configure, manage and operate their connection to the POI. As discussed in section 5.2.4, the demarcation point is at the POI side of the telecommunication facilities. Thus, the circuit is the Customer's responsibility, while the circuit termination equipment at the POI is the CNO responsibility.

Each circuit terminates on either an ATM switch, or the network side of a DSU/CSU, both of which are directly connected to the POI router. No additional functionality would be gained by a customer co-located router.

5.1.2.2 Subscriber Management Demarcation Point

This is the point at which operational management of the Subscriber transitions from the CNO to the Customer. This point is the Cable Modem (CM) Ethernet interface. The cable modem is the operational responsibility of the CNO, while the connecting cabling and the PC itself are the operational responsibility of the Customer.

This demarcation point location was selected due to:

- the potential operational impact on the network resulting from CM mis-configuration;
- the role of the CM in establishing service parameters on a shared data network; and
- the intrinsic role of the CM in the RF network management process.

The cable network appears to be an Ethernet from the data perspective. In fact, it is a Frequency Division Multiplexed (FDM) Radio Frequency (RF) network, utilizing the Data over Cable (DOCSIS) RF encoding system, with many active elements such as RF amplifiers and Amplitude Modulated (AM) lasers throughout the system. All RF signals are delivered right up to the CM, and the CM is configured as to which frequencies to receive and transmit on. Other RF sections carry management information for the video distribution system. Should the CM be mis-configured, significant operational disruption to the data and/or video distribution system could result. Thus, configuration of the modem must be the CNO's responsibility to ensure the integrity of the network.

The CM, once configured, establishes and enforces the service parameters delivered to the Subscriber. To ensure a fair system for each Customer, each Subscriber of each Customer must be assured of their service level commitment, and protected from Subscribers or Customers who would attempt to gain an unfair share of the shared data network. This behavior would endanger service deliverables and threaten the integrity of the network itself due to overload and/or misuse. As the CNO has final responsibility at the IP layer to fulfill service level commitments fairly to all third party Customers, it must have the ability to control the service parameters on a per Subscriber basis.

The CM is an intrinsic component of the CNO operational capability – the "smart jack" of the cable hybrid fiber-coaxial (HFC) network. The management demarcation point selection reflects this critical role of the CM in the CNO management process. The CM permits the CNO to detect RF plant problems through the use of embedded spectrum analyzer features, specialized error counters and RF level information. Without full management control of the CM, the CNO will be unable to proactively manage the RF plant, and it will have no recourse available to diagnose and resolve plant problems when experienced by the Customer and Subscriber. A CM not under the CNO's control effectively renders the Subscriber invisible to the CNO. As a result, the CNO must have full operational control of the CM.

5.1.2.3 Subscriber Provisioning Demarcation Point

The Subscriber provisioning demarcation point is the point closest to the subscriber at which the CNO will actively configure equipment. This demarcation point is established within the Subscriber's PC, namely at the IP stack configuration. Using the DHCP protocol, discussed in section 5.6, the Subscriber PC is provided with basic network layer configuration information. The Customer is responsible for all other configuration of the Subscriber PC.

It is important to separate the business process of deciding what configuration information should be communicated to the Subscriber PC and the technical mechanism for delivery of that information to the Subscriber PC. In this document, we deal with the technical mechanism of delivery only.

The demarcation point was selected due to:

- the need for a single DHCP server administration;
- the need to ensure a unique relationship between IP address and MAC address; and
- the need to coordinate multiple users of IP address space.

Each RSAN must have one or more DHCP servers to provide DHCP service. These DHCP servers each return a response to the Subscriber PC query. To ensure that the same response is returned, there must be coordination between the DHCP servers in some form, either technical or administrative. If there is no coordination, the system risks returning multiple, conflicting answers. As conflicting answers endanger the operational integrity of the network, there must be only one administrative authority for the DHCP server infrastructure. In particular, this means that Customers may not provide their own DHCP server infrastructure.

Multiple blocks of IP address space are typically used within each RSAN, generally one or more blocks per Customer. Each IP address must have only one MAC address, and each MAC address must have only one IP address. Without this assurance, Subscribers may be transitioned from one Customer to another without authorization. A single DHCP administrator provides the assurance that this will not happen.

As multiple customers are using the RSAN, there may be multiple understandings of which Customer has what IP address blocks, and which customers are assigned to them. A single DHCP administrative entity ensures that all parties are treated fairly, that problems are reconciled in advance of use on the network, and that the operational and administrative integrity of the network is protected.

5.2 Points Of Interconnection

A Point Of Interconnection (POI) is a place where Customer networks are connected to the CNO's network. Each potential Subscriber is served exclusively by one POI, so in order to provide service to that potential Subscriber the Customer must be connected to that POI.

5.2.1 POI Coverage

The geographic area and number of potential Subscribers served by each POI will be determined by the CNOs. Depending on how the CNO's network has been engineered, one POI may serve multiple cities, or one city may be served by multiple POIs. POI coverage information will be made available by the CNO to its Customers.

5.2.2 POI Location

The CNO may choose to locate a POI in a regional hub, in a primary hub (as pictured in Figure 5.1), or even in a secondary hub.

5.2.3 Customer connections to POIs

Each Customer may connect to multiple POIs, and multiple Customers may connect to each POI. The CNO provides, manages and operates the POI router. The Customer is allocated a port on the POI router for an RSAN when the CNO receives an order for Equal Access services at that RSAN.

5.2.4 Demarcation Point

For Asynchronous Transfer Mode (ATM) access, the demarcation for the CNO's operational responsibility is the carrier-end of the ATM network access to the POI. For dedicated line access, the demarcation point is the WAN side of a CNO supplied CSU/DSU attached to a port on the POI router.

5.3 IP Addressing

5.3.1 Addressing plan

Customer ISPs will provide the CNO with blocks of world routable IP addresses to be used in each RSAN. IP addresses are assigned to individual Subscribers by the CNO at provisioning time. Subscriber machines will acquire an address via DHCP at boot time and will retain it for as long as they are powered up. Except as required by addressing reorganizations (renumbering), Subscriber PC's will be assigned the same IP address each time they boot.

5.3.2 Allocation Issues

5.3.2.1 CIDR Block Allocation

World routable CIDR blocks are allocated by the Customers to the CNO for use on specific RSANs. Customers are responsible for ensuring that sufficient addresses are available for their Subscribers in each RSAN. Note that not all addresses in a CIDR block are available for Subscribers. Details about this may be found in section 5.3.2.3.

It is the Customer's responsibility to ensure that forward and reverse domain name service has been established for all addresses within a CIDR block before allocating it to the CNO. The CNO may refuse to make use of a CIDR block for which this has not been done.

5.3.2.2 CIDR Block Utilization

The CNO will assign individual IP addresses from each CIDR block to Subscribers of the Customer that provided that CIDR block. Not all addresses in a CIDR block will be available for assignment to Subscribers. The following addresses will be reserved for other uses:

- The lowest address within the CIDR block will be reserved for the default gateway

- The all 0s address will be reserved for broadcasts

- The all 1s address will be reserved for broadcasts

Additionally, the network architecture of some RSANs may require the CNO to subnet Customer provided CIDR blocks. If this is required then the above three addresses will be unavailable for Subscribers for each subnet within the CIDR block, resulting in a lower number of IP addresses available to Subscribers and introducing the possibility of address space fragmentation. For further information about this the Customer should contact the CNO.

5.3.2.3 Multiple CIDR Blocks

Because IP address renumbering (section 5.3.4) is best avoided when possible, CNOs may allow Customers to provide multiple CIDR blocks for use in one RSAN rather than requiring a renumbering each time additional address space is required. Because there is a limit on the number of subnets that the POI router can manage on one interface (to the RSAN) CNOs who do offer this service may still have to limit the number of total blocks available to a Customer before a renumbering is required to bring all of that Customer's Subscribers on a given RSAN into one, larger CIDR block.

5.3.2.4 Address Utilization Reporting

Customers are informed by the CNO as each new Subscriber is assigned an address, and in addition the CNO will send an address utilization summary to each Customer once each month. If the CNO subnets a Customer-provided CIDR block then the CNO will:

- Inform the Customer about the details of the subnetting when the subnets are created

- Report monthly on address utilization on a per subnet basis

If ever the CNO has assigned all the addresses allocated to it for an RSAN or portion thereof by a Customer it will immediately inform that Customer, making it clear that further subscriptions in that area will not be possible until additional address space has been provided. The above notwithstanding, it is the responsibility of the Customer to ensure that the CNO has been allocated sufficient address space to serve the Customer's Subscribers.

5.3.3 Assignment Methodology

Subscribers are assigned an IP address, from the CIDR block provided by the Customer chosen by the Subscriber, by the CNO when the Subscriber is first provisioned. The Subscriber will retain that same address until service is terminated, or until re-allocation of CIDR blocks requires a renumbering.

5.3.4 IP Address Renumbering

It may be necessary on an infrequent basis to change the IP addresses assigned to a group of Subscribers in order to restructure the address allocation. The following issues must be considered:

- The change will be transparent to Subscribers not using the service at the time of the renumbering, therefore the renumbering should be done when usage is at it's lowest, probably between 2:00am and 4:00 am on a weekday.

- Currently available PC implementations of DHCP do not allow for their IP address to be changed after it is initially set at boot time. Affected Subscribers should therefore be informed via email that if their PC is in use during the time of the renumbering it may lose connectivity. If this happens, a simple reboot will re-establish internet connectivity.

- Although Subscriber IP addresses will change, their domain names should not. In the time preceding the renumbering, DNS servers for Subscriber domain names/addresses should not send out replies with a TTL which extends past the time of the renumbering. Usual TTLs may immediately be used again after the renumbering is complete and the DNS database is updated with the new A records.

  Because the DNS is maintained by the Customer and the IP address renumbering will be performed by the CNO, careful coordination between the two will be required. Specifically the Customer will require advance notice of the following: What is the address range which will be affected? What will the new addresses be? How will old address be mapped to new addresses? Exactly when will the renumbering occur?

5.3.5 Cable Modem Addressing

Cable modems are assigned private addresses by the CNO and are not visible to Customers or Subscribers. Private addressing space is used to ensure IP address density requirements are met for future address space applications, and to adhere to INTERNIC/IANA guidelines with respect to cable networks.

5.4 Routing

Routing of packets to Subscribers is made simple by the use of world routable address blocks. The Subscriber's ISP is responsible for routing Subscriber-destined packets to the appropriate POI router, which forwards them to the Subscriber via the DOCS using statically configured routes.

Routing packets from the Subscriber to the world at large is slightly more complicated because the path taken by the packet must depend not on where it is going, as is usual, but which Customer's Subscriber sent it. This is accomplished by having the POI routers route each packet to the appropriate Customer based on source address rather than destination address. The Customer then forwards the packet in the usual way.

The POI router does not exchange routing information with connected Customer routers. Customer routers must maintain static routes to reach their CNO served Subscribers, and the POI router will be configured with static routes for each Customer provided CIDR block. Configured routes should be conditional on link status.

POI routers are explicitly not transit points between Customers. Traffic generated by a Subscriber for an address served by a different Customer on the same RSAN will be routed to the Subscriber's ISP, not the ISP responsible for the destination address.

5.5 DNS

Both forward and reverse domain name service will be provided by the Customer. Both will be in place for each CIDR block allocated to the CNO before such allocation.

Assignment of domain names to IP addresses will be done by the Customer before the CIDR block is allocated to the CNO. Because of this, no DNS updates are required as subscribers are added or dropped, and co-ordination between the Customer and the CNO is not necessary.

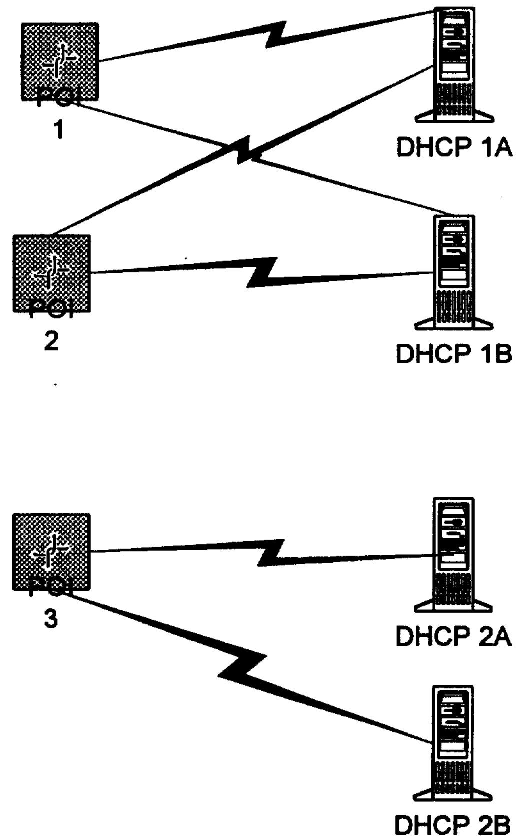
Because all domain name services are provided by the Customer, the Customer will be able to provide vanity domain names to its Subscribers without involvement of the CNO, should it choose to do so.

5.6 DHCP

DHCP is used to configure network parameters for both CMs and Subscriber PCs. Provision and operation of DHCP servers is the responsibility of the CNO.

5.6.1 DHCP Architecture

This document generally refers to the simplest case, where one DHCP service provides service to all the CNO's RSANS via an internal network, possibly an incumbent network. It is also possible, at the CNO's discretion, for multiple servers to be used together in order to provide redundancy and/or load sharing.



• Figure 5.2 DHCP Architecture showing redundancy and load sharing

5.6.1.1 DHCP Redundancy

DHCP server redundancy can be achieved by configuring the POI routers to be aware of more than one DHCP server. The POI router will then forward DHCP requests from Subscriber PCs and CMs to all of the servers it is aware of, and will return all replies to the DHCP client device.

DHCP clients must be able to handle multiple responses to a request as documented in RFC 1541. The CNO shall ensure that where multiple DHCP servers respond to a client, the responses shall be identical with respect to the network configuration information required by the clients.

Figure 5.2 shows redundant DHCP service being provided to POI routers 1 and 2 by DHCP servers 1A and 1B, and to POI router 3 by DHCP servers 2A and 2B

5.6.1.2 DHCP Load Sharing

If performance issues make it desirable to split the DHCP load between multiple servers, or if there is not a suitable communications channel between all parts of the CNOs DOCS infrastructure to make the operation of a single centralized DHCP server practical, then the CNO may choose to divide its DOCS infrastructure into multiple DHCP serving areas.

If this is done:

- Each POI router must be configured to forward DHCP requests to the DHCP server(s) serving the DHCP serving area which it is part of.

- The database used by the DHCP servers to map CM and PC MAC addresses to network parameters must be distributed in whole (for ease of implementation) or in part (for efficiency) to the DHCP servers at intervals no longer than the maximum acceptable time between assigning an IP address to a new Customer and providing service to that Customer. Ideally, changes to this database will be replicated in real time.

If the DHCP server databases are distributed in whole, then each server will have information required for all service areas, not only the one it operates in. This may result in a small, possibly inconsequential performance penalty.

Alternatively, each server may be updated only with the information relevant to its serving area. Redundant servers in a single serving area must still have identical databases.

In the example illustrated by Figure 5.2, the DOCS infrastructure has been divided into two serving areas. The first, containing POI routers 1 and 2, is redundantly served by DHCP servers 1A and 1B. The second, containing only the single POI router 3, is redundantly served by DHCP servers 2A and 2B.

5.6.2 DHCP and Subscriber PCs

Customers will assist their Subscribers in installing DHCP software on their PC so that the Subscriber's IP address and other network parameters can be set by DHCP at boot time.

The parameter provided to the PC via DHCP will be the following:

- IP address
- IP network mask
- IP default gateway
- IP address of Domain Name server

5.6.3 DHCP and Cable Modems

Cable modems acquire their network parameters at boot time via the same DHCP server used to service Subscriber PCs. This is transparent to both Customers and Subscribers.

5.6.4 Tracking of Subscriber And CM MAC Addresses

DHCP may be configured to identify and allocate IP addresses to clients (CMs and PCs) either by the client's MAC address, or by a "Client-ID" manually configured in the device. Each approach has its strengths and challenges. Standard practice today is to use the MAC addresses, and this document assumes that practice.

This approach ties client identification to physical rather than logical components. The CNO must keep accurate information about which Customers have which physical cable modems in order to keep the CM entries up to date in the DHCP database.

Similarly, the CNO must keep track of the MAC address of the NIC in the Subscriber's PC, and must make Subscribers aware that any NIC changes must be coordinated with the CNO, or the Subscriber will lose connectivity.

5.7 PC Network Configuration

The Customer is responsible for ensuring that its Customers PCs are correctly configured for TPRIA service beyond the provisioning demarcation point. This includes installation and configuration of a compatible DHCP client, as well as application specific software such as email, web browsing, Usenet news, etc. Proper installation of these applications may include the configuration of Subscriber identification information such as name and email address, domain names of servers associated with the application (NNTP, SMTP, POP3, etc.) etc.

The CNO may require the use of DHCP client software which it has determined is compatible with the TPRIA service.

The CNO is responsible for responding to Subscriber DHCP request with the information detailed in section 5.6.2

5.8 Modem Network Configuration

Modem configuration and management is the responsibility of the CNO. Modem configuration is provided by the CNO DHCP and TFTP servers in accordance with DOCSIS cable modem specifications.

The CNO may implement the business policies that are reflected in the cable modem configuration. Examples may include port filters, speed limits, etc.

5.9 ARP

ARP requests are intercepted and answered by the CMTS. ARP requests are not seen by other devices on the DOCS.

6 Operational Analysis

6.1 Device Startup

6.1.1 Modem boot

When a cable modem boots it starts by broadcasting a DHCP request from its cable port. This request is forwarded by the CMTS (if it is routing) or the POI router (if the CMTS is not routing) to the DHCP server, and the reply is sent back to the CM. This reply contains the information that the CM needs to establish basic IP connectivity.

Next the CM connects to a TFTP server maintained by the CNO and downloads the rest of its configuration from there. When that has completed the CM is ready to bridge packets to and from the Subscriber's PC.

6.1.2 PC Boot

The Subscriber's PC should be booted only when the cable modem is operating.

When the Subscriber's PC has booted, it broadcasts a DHCP request on the Subscriber's Ethernet LAN. The CM bridges that broadcast to the DOCS, where it is picked up by the POI Router or CMTS (as in 6.1) and the response is sent back to the Subscriber's PC.

6.2 Unicast Packet Flow

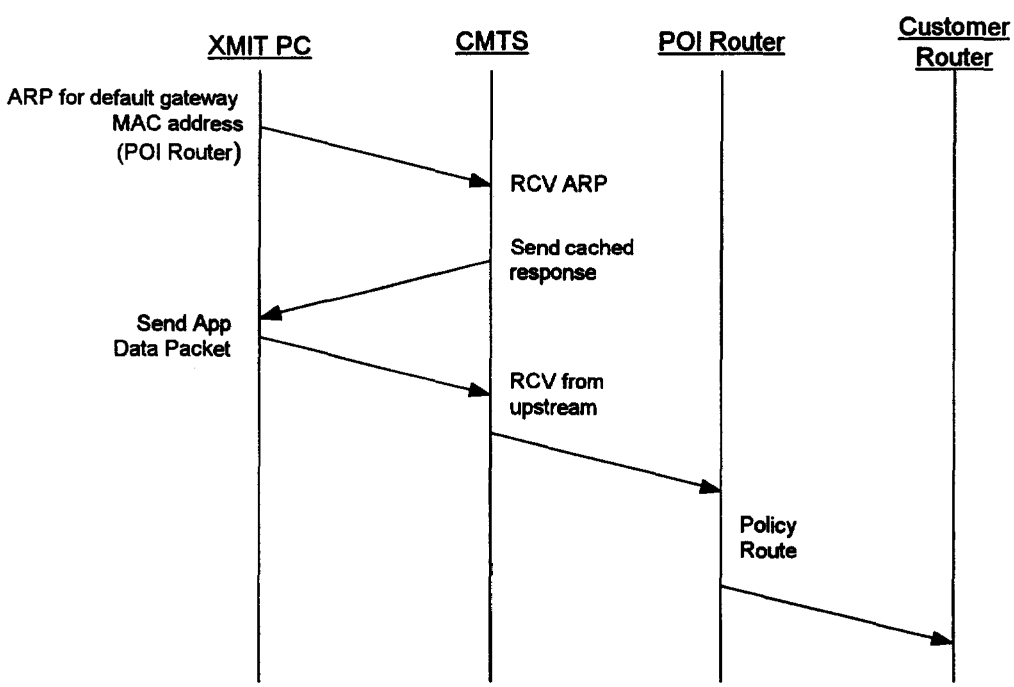
6.2.1 Internet to Subscriber

Packets from the public Internet are routed to the Subscriber's ISP in the usual fashion. The ISP maintains static routes for each POI to which it connects. The POI router maintains an ARP table used to send each packet to the appropriate Subscriber.

6.2.2 Subscriber to Internet

The Subscriber's PC sends Internet-destined packets to its default gateway which is the POI router if the CMTS is configured as a bridge, or the CMTS itself if it is configured as a router. In the latter case, the CMTS passes the packet back to the POI router.

The POI router examines the source address of each incoming packet, determines which CIDR block it is part of, and sends the packet to the Customer which allocated that CIDR block to the CNO. The Customer routes the packet to the public Internet.

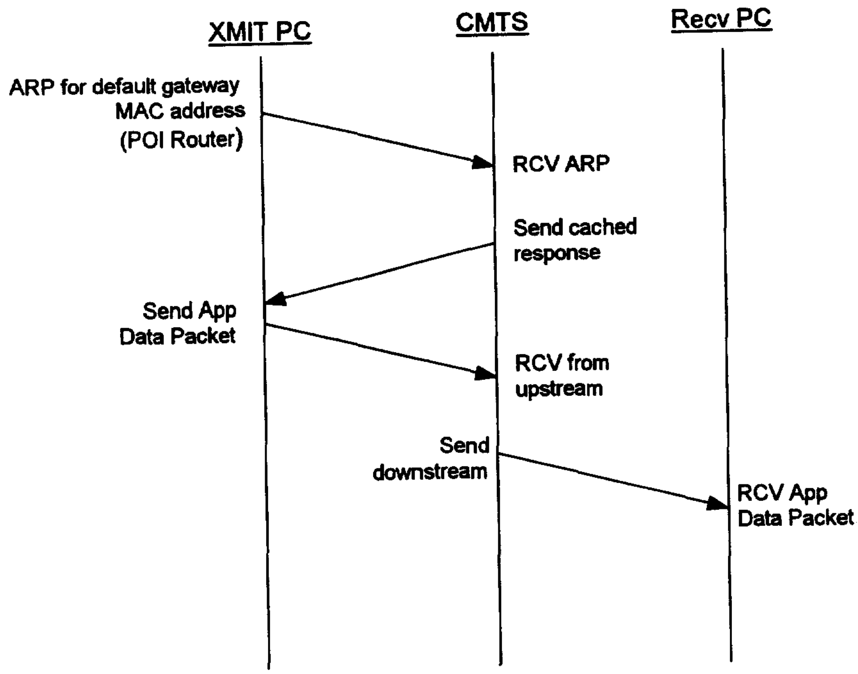


• Figure 6.1 Subscriber to Internet

6.2.3 Subscriber to Subscriber (Same ISP)

Subscribers who are Customers of the same ISP and served by the same RSAN may or may not be on the same subnet.

If they are on the same subnet then the process looks like this:

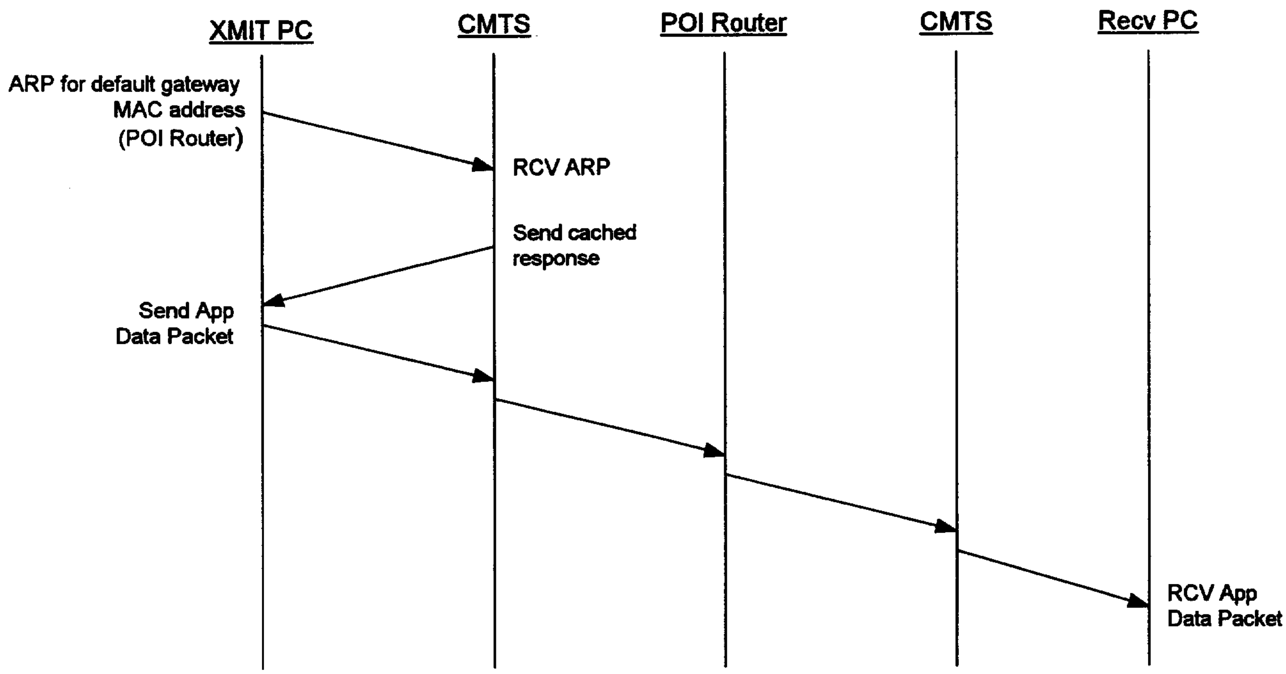


• Figure 6.2 Subscriber to Subscriber - Same ISP

If the ISP has provided more than one subnet for use on the RSAN then it is possible for two Subscribers of one ISP, on one RSAN, to be on different subnets. That case is functionally identical to the instance of two Subscribers of different ISPS on one RSAN, described in section 6.2.4.

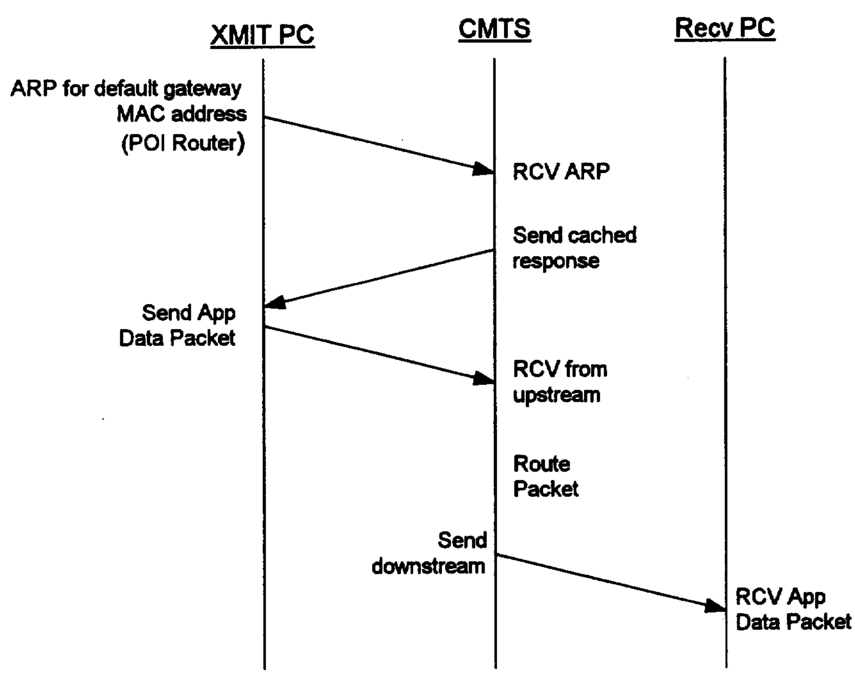
6.2.4 Subscriber to Subscriber (Different ISPs)

The CMTS on an RSAN may be configured to operate as a bridge or as a router. If the CMTS is configured as a bridge then the process looks like this:



• Figure 6.3 Different ISP, Bridged

If the CMTS is configured to act as a router then the process looks like this:



• Figure 6.4 Different ISP - Routed

6.2.5 Subscriber to Non-Subscriber (Same ISP)

This is functionally equivalent to 6.2.2. There is no special handling for this case.

6.2.6 Subscriber to Non-Subscriber (Different ISP)

This is functionally equivalent to 6.2.2. There is no special handling for this case, even if the destination ISP is directly connected to the Subscribers POI router the packet will still be routed to the Subscriber's ISP.

6.3 Broadcast Packet Flow

Careful consideration must be given to the handling of broadcast traffic. Unrestricted broadcast leaves the network open to denial of service at the very least, but some broadcast ability is necessary to make possible required protocols such as ARP and DHCP.

It is essential that the CMs filter replies from Subscriber PCs to DHCP requests.

It is strongly recommended that the CMs also filter all broadcasts out from Subscriber PCs except ARP and DHCP, and **all** broadcasts in to Subscriber PCs.

6.4 Multicast Packet Flow

Multicast IP is not supported by this product.

CCTA Submission to CRTC
In Response to Telecom Decision 98-9

Technical Report on the Status of Implementation of Access For Internet Service Providers

1. This report outlines the status of implementation of access to the cable network operators' high-speed Internet subscribers by competitive Internet service providers. The report provides an update on technical progress made since the CCTA's August 10 report to the Commission.

2. The report reviews the technical decisions taken by the CAIP/CCTA working group, which consists of representatives from Internet service providers and from the cable industry. The technical working group meetings have also been attended by CRTC staff representatives. Significant progress toward the implementation of third-party residential Internet access has been achieved over the last three months through open and productive technical discussions.

3. For reference, a diagram has been provided on page 3 showing the cable network operators' access infrastructure as used for the delivery of Internet services. This diagram depicts interconnection to third party ISPs through a policy-based router.

4. The technical solution for interconnection is being developed specifically to support the Canadian requirement, in the absence of a regulatory requirement for interconnection to cable network operators' networks in any other jurisdiction.

Technical Work in Progress

5. As mentioned in the August 10 report, there are three key areas of technical development in support of the implementation of access by competitive ISPs. The first of these is the availability of industry standard DOCSIS modems. The second is the development and testing of appropriate technology at the router point of interconnection (POI). The third is the development and testing of implementation plans that reflect the business processes to support the deployment of commercial service.

DOCSIS Modem Availability

6. DOCSIS version 1.0 cable modems and cable modem termination systems are in the process of certification testing overseen by CableLabs, the research and development arm of the North American cable industry. Some Canadian cable network operators have begun deployment of pre-certification DOCSIS modems from manufacturers and are already performing field tests. These companies will be well positioned to quickly roll out the certified DOCSIS products once they

become available. Volume rollout of certified DOCSIS modems is expected in 1999.

Point of Interconnection

7. The work of the CAIP/CCTA technical group for the last three months has focussed on the point of interconnection. At the August 25 meeting, the alternatives presented in the CCTA August 24 report to the CRTC were discussed. These options were:

   1. VLAN
   2. IP Tunneling
   3. Policy-Based Routing
   4. User-Driven Policy-Based Routing

8. The group decided to review the pros and cons of the four options at its next meeting.

9. At the September 22 meeting of the CAIP/CCTA technical working group, an analysis of the four technical options was reviewed. After considerable discussion, it was decided that the policy-based routing option had the best chance of a successful implementation, confirming the CCTA's original recommendation.

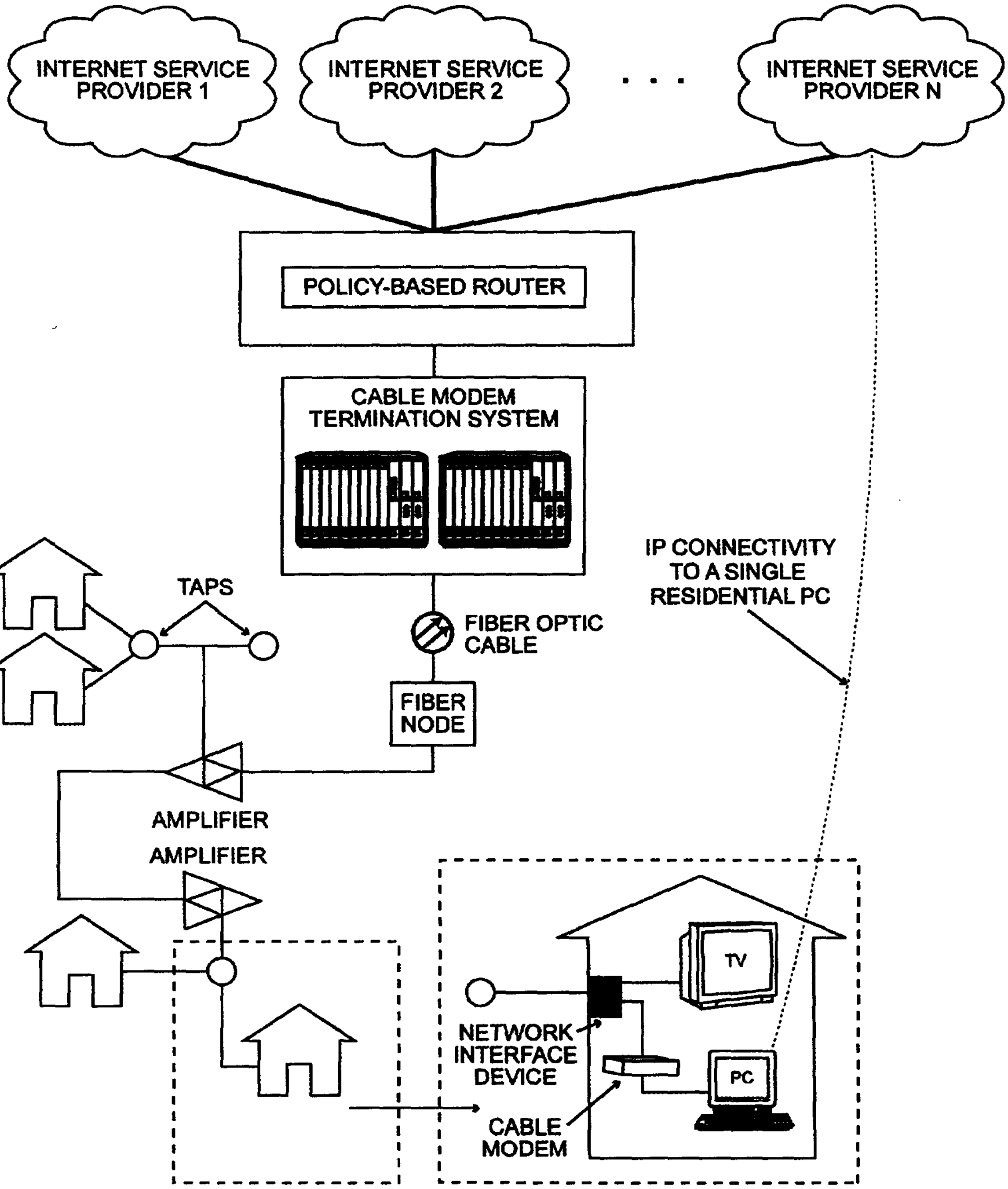
10. Once the fundamental technology at the point of interconnection was confirmed, the group decided to proceed with a network design for the point of interconnection. This is a key subsystem in the current plan for interconnection. A sub-working group consisting of representatives from Netcom, Tekton Internet Associates and the CCTA was formed to create a proposal for consideration by the rest of the group.

11. The sub-working group met on October 7 and October 16 for the purpose of reviewing and editing a draft network design created by Tekton Internet Associates on behalf of the CCTA. Most of the discussion concerned the location of the provisioning and management demarcation points.

12. The draft version of the report was presented to the entire CAIP/CCTA technical group at a meeting on October 20. At that time, members of the sub-working group answered questions from the group as to the specific reasoning for design decisions taken. The group then approved the design. The consensus document is appended to this report.

13. Also at the October 20 meeting, the CAIP/CCTA group tasked the same sub-working group to prepare a test plan for the router point of interconnection. This test plan is to be developed at team meetings to be held on November 2, November 6 and November 13. It will be reviewed at the meeting of the CAIP/CCTA group on November 17.

14. Once the test plan is approved, testing of the router point of interconnection can begin. This relatively new technology has not been used before in a cable network for high-speed Internet access. The viability of this alternative for interconnection must be verified in a laboratory setting. Work will continue in parallel on the development of business processes for interconnection.



Development of Business Processes

15. At the October 20 CAIP/CCTA meeting, CCTA presented a timetable for the development of business processes toward implementation of third party access. In order to accelerate the process, a two-track schedule has been developed.

16. A flowchart showing the two-track schedule for testing and design is presented on page 5 of this report, including target dates for starting and finishing each stage.

17. The schedule has a design track and a testing track. The testing track is to begin in November with the testing of the router point of interconnection. During this stage, the policy-based router design for the point of interconnected will be tested.

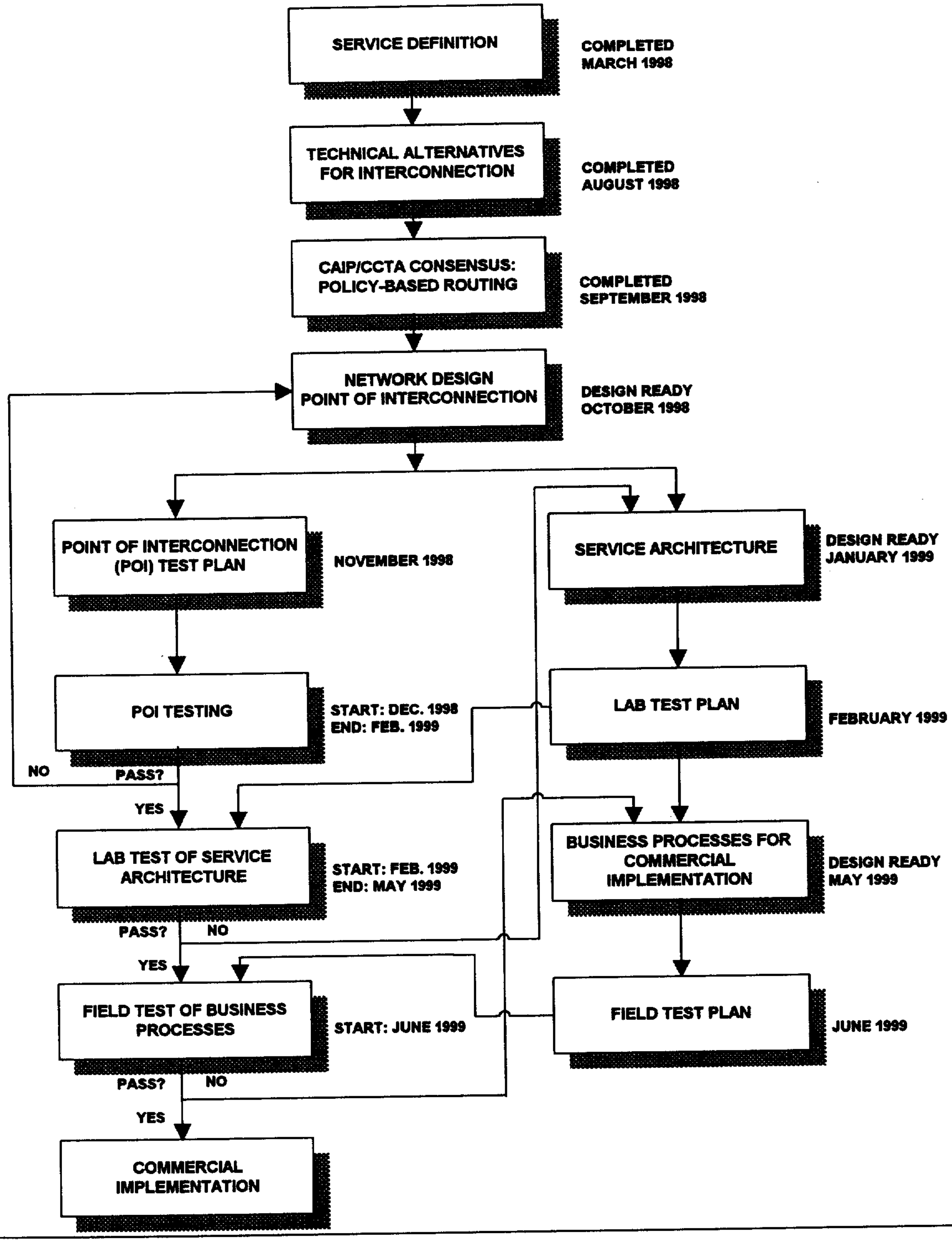
18. The second phase of testing involves a captive laboratory test of the provisioning system to be used by the ISPs and the cable network operator. During this phase, no live cable modem subscribers will be interconnected but a cable network operator will connect remotely to an ISP test system and will provision subscriber PCs in the lab.

19. The third phase of testing will use equipment in the field, connected to a cable network operator's live network. The CNO will interface to an ISP using the processes that are to be used in the commercial implementation.

20. The design track, which is to proceed in parallel with the testing track, begins with the development of the service architecture. The service architecture, and its associated test plan, are inputs to the lab test plan.

21. The next stage in the design track is the development of business processes to support commercial implementation and the associated test plan for these processes. These are the inputs to the field testing. It is important to note that this phase is likely to require significant modifications to the cable network operators' existing information technology infrastructure.

22. With the successful completion of the field test, both Internet service providers and cable network operators will gain confidence in the business processes designed for commercial deployment of third party access.



SERVICE DEFINITION
COMPLETED MARCH 1998
TECHNICAL ALTERNATIVES FOR INTERCONNECTION
COMPLETED AUGUST 1998
CAIP/CCTA CONSENSUS: POLICY-BASED ROUTING
COMPLETED SEPTEMBER 1998
NETWORK DESIGN POINT OF INTERCONNECTION
DESIGN READY OCTOBER 1998
POINT OF INTERCONNECTION (POI) TEST PLAN
NOVEMBER 1998
SERVICE ARCHITECTURE
DESIGN READY JANUARY 1999
POI TESTING
START: DEC. 1998 END: FEB. 1999
LAB TEST PLAN
FEBRUARY 1999
NO
PASS?
YES
LAB TEST OF SERVICE ARCHITECTURE
START: FEB. 1999 END: MAY 1999
BUSINESS PROCESSES FOR COMMERCIAL IMPLEMENTATION
DESIGN READY MAY 1999
PASS?
NO
YES
FIELD TEST OF BUSINESS PROCESSES
START: JUNE 1999
FIELD TEST PLAN
JUNE 1999
PASS?
NO
YES
COMMERCIAL IMPLEMENTATION

Summary and Next Steps

23. The CAIP/CCTA technical group has made significant progress toward the implementation of third party access to cable network operators' high-speed Internet subscribers. The method of interconnection has been selected, and a network design for that point of interconnection has been approved.

24. The next steps for the group are the development of a test plan for the point of interconnection, and the execution of the test of that point of interconnection. In parallel, the service architecture will be developed.

25. The progress of the CAIP/CCTA technical group can be attributed to a clear focus on the task at hand by a group of representatives who are oriented to making third party access a reality. The group represents the most efficient mechanism for the development of business processes to support third party access.